Statement of William E. Gray
Deputy Commissioner
Office of Systems
of the
Social Security Administration
Before the
Committee on Government Reform
June 8, 2006

Mr. Chairman and Members of the Committee, thank you for inviting me here today to discuss government data security at the Social Security Administration (SSA). Commissioner Barnhart and I place the highest importance on our information security program and are committed to securing and protecting Federal information. As SSA's Deputy Commissioner for Systems, I appreciate the opportunity to discuss our data security policies and procedures with you this morning.

At SSA we have always recognized the importance of protecting the security and privacy of the people we serve and ensuring the integrity and accuracy of the records we maintain. As you know, Mr. Chairman, the Social Security Board's first regulation, published in 1937, dealt with the confidentiality of SSA records. Our policies predate and are consistent with the Privacy Act. For more than 70 years, since long before the advent of computers and the technology age, SSA has honored its commitment to the American people in maintaining the confidentiality of our records. Our emphasis on privacy has led to a strong commitment in data security.

At SSA, we use a variety of inter-related, proactive measures to protect the information that the American public entrusts with us. These include physical security measures, Information Technology (IT) security measures, and training

and security protections for our employees. We have tried to put in place the authorities, the personnel, and the software controls to prevent penetration of our systems and to address systems security issues as they surface.

Prevention of Unauthorized Access

We use state-of-the-art software that carefully restricts user access to data. Using this software, only persons with a "need to know" to perform a particular job function are approved and granted access to specific kinds of data. All access to our mainframe computer is controlled through this matrix access process, also known as “Top Secret Services”.

These systems controls not only register and record access, but also determine what functions a person can do once access is authorized. SSA security personnel assign a computer-generated personal identification number and an initial password to persons who are approved for access (the person must change the password every 30 days). This allows SSA to audit and monitor the actions individual employees take when using the system. These same systems provide a means to investigate allegations of misuse and have been crucial in prosecuting employees who misuse their authority.

Additionally, we have implemented processes to scan, at least once a month, every SSA workstation (over 100,000), every telephone, and every systems platform for compliance with Agency standards. I believe that our record in preventing intrusions demonstrates our success in implementing an Enterprise-wide security program that is second to none.

Prevention of unauthorized access is enhanced by risk assessments, systems penetration testing, physical safeguards, and independent audits and reviews.

Human Capital

We nurture a security-conscious culture throughout the agency from the executive level down.

For instance, every time any SSA employee, and that includes the Commissioner of Social Security, logs onto his or her workstation, a banner pops up warning that only authorized users can access the system; that the system is a United States government computer system subject to Federal law, and that unauthorized attempts to access, upload, or otherwise alter SSA's data or programming language are strictly prohibited and subject to disciplinary and/or civil action and criminal prosecution. In effect, every SSA employee sees that message every day he or she comes to work.

And as you may know, every year, every SSA employee must read the Sanctions for Unauthorized Systems Access Violations (Sanctions) which we developed to secure the integrity and privacy of personal information contained in the Agency's computer systems. This memorandum advises SSA employees of the categories of systems security violations and the minimum recommended sanctions. These sanctions apply for all SSA employees who use or have access to computer systems containing personal data about workers, claimants, beneficiaries, SSA employees or other individuals. Annually, all employees are required to read and sign the Acknowledgment Statement indicating that they have read and understand the sanctions. The Sanctions and Acknowledgment Statement have both been incorporated into the Information Systems Security Handbook.

We are also very serious about training. We provide security awareness training to all of our employees (including contractors) and specialized in-depth training for those with significant IT security responsibilities. Contractors are required to possess security credentials, and have the expertise and training appropriate to the functions they will be performing before they are permitted to perform services under a contract.

In addition, we have networks of full-time staff devoted to systems security stationed throughout the Agency. These front-line employees provide day-to-day oversight and control over our computer software in headquarters and centers for security and integrity in each SSA region.

IT Security Measures

We closely follow Federal guidelines including security standards and guidelines issued by the National Institute of Standards and Technology (NIST) and the Office of Management and Budget. We incorporate these standards and guidance into Agency policy for information security and the related Certification and Accreditation (C&A) of our major IT systems. The C&A process is a major part of our efforts to maintain and strengthen our systems controls.

And as we reported to you this past March, we use the Federal Information Security Management Act (FISMA) reporting process as an important indicator of how the agency's information technology assets and resources are being protected. SSA submitted our report for fiscal year 2005 to OMB on October 7, 2005. A few of the major highlights of our report are especially relevant to today's discussion. For example, we reported to you that all twenty of our major information systems are currently certified and accredited. We follow documented policies and procedures for identifying and reporting incidents of security weakness and use a combination of automated tools, system monitoring tools and network-penetration type reviews to protect all 20 of our information systems. And, as required by NIST, SSA provides monthly incident reports to the United States Computer Emergency Readiness Team.

Flexiplace at SSA

Consistent with May 2003 guidance from the Office of Personnel Management (OPM), we have a flexiplace program in place at SSA that we are now obligated to maintain under our collective bargaining agreements. All participating employees are required to sign, and abide by, their individual component's negotiated Flexiplace Program Participant Agreement. Of our current workforce of 64,000 employees, 4,400 have signed flexiplace agreements. These agreements require adherence to applicable government regulations in place at SSA governing information management and electronic security procedures for safeguarding data and data bases. While each flexiplace agreement is different, they share certain basic requirements. Regarding security, the agreements generally contain provisions that:

- require participating employees to maintain lockable storage for securing files at the alternate duty site;

- require participating employees to protect government records from unauthorized access, theft, damage in addition to requiring protection from unauthorized disclosure in accordance with the Privacy Act and other federal laws restricting disclosure of the information we maintain; and

- allow for management inspection of the alternate duty station with 24 hours advance notice to the employee.

A violation of the conditions I have just laid out results in disciplinary action. Penalties may range from reprimand to removal, depending on the seriousness of the violation. Despite our best efforts in establishing policy and procedures and in enforcing these procedures, no system of safeguards is immune from human error. We use these rare occurrences to review and strengthen our security precautions. Recently a laptop computer owned by an SSA employee

was stolen from a conference the employee was attending. The laptop contained copies of decisions the employee had written as part of his assigned work when he worked at home. There were approximately 200 files on the laptop that were stolen and these files contained the names, Social Security numbers and other personal information pertaining to these individuals. While the investigation is still underway, we have taken steps to notify the individuals whose files were contained on the laptop and to monitor the SSNs to ensure no suspicious activity has occurred on SSA's records. This employee, although authorized to work at home, violated SSA security procedures by failing to properly secure sensitive information on the laptop, and by taking it to a non-secure location.

Detection of SSN Misuse

As recent experience makes clear, despite government's best efforts to protect data, breaches do occur. So I would like to turn now to a discussion about detecting SSN misuse.

One way that a person can find out whether someone else is misusing their number to work is to check his or her earning records. About three months before their birthday, anyone 25 or older and not already receiving Social Security benefits, automatically receives a Social Security statement each year. The statement lists earnings posted to their Social Security record and provides an estimate of benefits and other Social Security facts about the program. If there is a mistake in the earnings posted the individual is asked to contact us right away, so the record can be corrected. We investigate, correct the earnings record and if appropriate, we refer any suspected misuse of a Social Security number to the appropriate authorities.

SSA may learn about misused SSNs in a variety of other ways including alerts from our computer systems while matching Federal and State data, processing wages, claims or post entitlement actions, reports from individuals contacting our field offices or teleservice centers and inquiries from the Internal Revenue Service concerning two or more individuals with the same SSN on their income tax returns.

We have another tool that has been used successfully to detect instances of fraud and abuse. This tool, called the Comprehensive Integrity Review Process (CIRP), is a review and anomaly detection system. Known fraudulent patterns are first identified and then transactions that fit these fraudulent patterns are provided to SSA managers for their review. If upon investigation, the SSA manager believes that fraud or misuse has occurred, they prepare a referral to the Inspector General (IG).

As I have tried to make clear today, our approach to data security is multi-faceted, and involves numerous policy, hardware and software safeguards. However, even with all the measures and safeguards we use, we cannot rest and be satisfied that we have plugged every hole. The challenge is to keep ahead of threats with an intense and responsive security program. We continue to monitor, test and evaluate what we are doing to prevent, detect, and mitigate any potential threat. We strive to create and maintain a security conscious culture; we continue to try to stay abreast of all threats and emerging technologies and vulnerabilities associated with those technologies, and our goal is to keep up with "best practice" approaches related to information security. We have recently reemphasized with all employees the critical importance of safeguarding personal information, and we have directed managers to reinforce this point with their employees. In light of recent events, we are also conducting a review of our response procedures and protocols.

Conclusion

Mr. Chairman, Commissioner Barnhart and I, along with all of the senior executives at the Social Security Administration, recognize data security is an ongoing challenge and critical component of our mission. We know we must be vigilant in every way to assure that an individual's personal information remains secure, taxpayer dollars are protected, and that public confidence in Social Security is maintained. We look forward to continuing to work with the Committee to assure the American people that we are doing all we can to maintain the security of the information entrusted to us.

Thank you for the opportunity to speak before this committee and I am happy to answer any questions.